CHAPTER 44

IPv6 ACL の設定

この章では、IE3000 スイッチに IPv6 ACL を設定する方法について説明します。IP バージョン 4（IPv4）の名前付き Access Control List（ACL; アクセス制御リスト）を作成して適用する方法と同様に、IPv6 ACL を作成してインターフェイスに適用することにより、IP バージョン 6（IPv6）トラフィックをフィルタリングできます。入力ルータの ACL を作成して適用することにより、レイヤ 3 管理トラフィックのフィルタリングもできます。

（注） IPv6 を使用するには、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定する必要があります。テンプレートを選択するには、**sdm prefer** {**default** | **dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力します。IPv6 の ACL をサポートするのは、IP サービス イメージが稼動しているスイッチだけです。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」を参照してください。
- スイッチの ACL の詳細については、第 44 章「IPv6 ACL の設定」を参照してください。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章の内容は次のとおりです。

IPv6 ACL の概要

スイッチ イメージは、2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL
  - レイヤ 3 インターフェイス（ルーテッド ポート、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel）のアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。
  - ルーティングされる IPv6 パケットだけに適用されます。

- IPv6 ポート ACL
  - レイヤ 2 インターフェイスのインバウンド トラフィックでだけサポートされます。
  - インターフェイスに着信するすべての IPv6 パケットに適用されます。

（注）　サポートされない IPv6 ACL を設定するとエラー メッセージが表示され、設定は有効になりません。

スイッチは、IPv6 トラフィックの VLAN ACL（VLAN マップ）をサポートしません。

（注）　スイッチでの ACL サポートについては、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。

1 つのインターフェイスに IPv4 と IPv6 両方の ACL を適用できます。

IPv4 ACL と同様に、IPv6 のポート ACL も、ルータ ACL より優先されます。

- 入力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信されたパケットには、ポートの ACL のフィルタが適用されます。他のポートで受信したルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータの ACL および入力ポートの ACL が SVI に存在している場合、ポートの ACL が適用されたポート上で受信されたパケットには、ポート ACL のフィルタが適用されます。発信するルーティング IPv6 パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

（注）　*いずれか*のポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

ここでは、スイッチの IPv6 ACL の特性について説明します。

- 「サポートされる ACL 機能」（P.44-2）
- 「IPv6 ACL の制限事項」（P.44-3）

サポートされる ACL 機能

スイッチの IPv6 ACL には、次の特性があります。

- フラグメント化されたフレーム（IPv4 では **fragments** キーワード）がサポートされます。
- IPv4 と同じ統計情報が IPv6 ACL でもサポートされます。
- スイッチの TCAM 領域が足りなくなると、ACL ラベルに関連付けられているパケットが CPU に転送され、ACL がソフトウェアで適用されます。
- ホップバイホップ オプション付きのルーテッド パケットおよびブリッジド パケットでは、IPv6 ACL がソフトウェアに適用されます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。

IPv6 ACL の制限事項

IPv4 では、番号付きの標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 では、名前付き ACL だけサポートされます。

スイッチでは、一部の例外を除いて、Cisco IOS でサポートされる IPv6 ACL の大部分がサポートされます。

- IPv6 送信元アドレスと宛先アドレス：ACL 照合は、Universal Identifier（EUI）-64 形式の /0 ～ /64 のプレフィクスと、ホスト アドレス（/128）でだけサポートされます。スイッチは、サポートする情報の損失のないホスト アドレスは次のものだけです。
  - 集約可能なグローバル ユニキャスト アドレス
  - リンクローカル アドレス
- スイッチは **flowlabel**、**routing header**、および **undetermined-transport** キーワードの照合をサポートしません。
- スイッチは再帰 ACL（**reflect** キーワード）をサポートしません。
- このリリースでは、IPv6 のポート ACL およびルータ ACL だけがサポートされます。VLAN ACL（VLAN マップ）はサポートされません。
- スイッチは、IPv6 フレームに MAC ベース ACL を適用しません。
- IPv6 のポート ACL は、レイヤ 2 EtherChannel に適用できません。
- スイッチは、出力ポートの ACL をサポートしません。
- IPv6 の出力ルータの ACL および入力ポートの ACL は、スイッチでだけサポートされます。スイッチは、コントロール プレーン（着信）の IPv6 ACL だけをサポートします。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限はありません。ハードウェア転送を必要とするインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、スイッチはそのインターフェイスで ACL がサポートされるかどうかを判別します。サポートされない場合、ACL の付加が拒否されます。
- ACL をインターフェイスに適用して、サポートされないキーワードを含む Access Control Entry（ACE; アクセス制御エントリ）を追加しようとすると、スイッチは現在そのインターフェイスに適用されている ACL にその ACE を追加することを許可しません。

IPv6 ACL の設定

IPv6 の ACL を設定する前に、デュアル IPv4/IPv6 SDM テンプレートのいずれかを選択する必要があります。

IPv6 トラフィックをフィルタリングする手順は、次のとおりです。

ステップ 1　IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

ステップ 2　IPv6 ACL でトラフィックをブロックする（拒否）か通過させる（許可）かを設定します。

ステップ 3　インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

ここでは、IPv6 ACL を設定して適用する手順について説明します。

- 「IPv6 ACL のデフォルト設定」（P.44-4）

IPv6 ACL のデフォルト設定

IPv6 ACL は設定または適用されていません。

他の機能との相互作用

IPv6 ACL の設定には、他の機能またはスイッチ特性と次の相互作用があります。

- IPv6 ルータの ACL がパケットを拒否するように設定されている場合、パケットは廃棄されます。パケットのコピーが Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ポート ACL によりブリッジド フレームが廃棄されると、そのフレームはブリッジされません。
- IPv4 と IPv6 の両方の ACL を 1 つのスイッチに作成して、両方の ACL を同じインターフェイスに適用できます。それぞれの ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するときに間違ったコマンドを使用すると（たとえば、IPv4 のコマンドを使って IPv6 ACL を付加しようとすると）、エラー メッセージが表示されます。
- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は、非 IP フレームだけをフィルタリングできます。
- TCAM が満杯の場合に設定済み ACL を追加すると、パケットが CPU に転送されて、ACL はソフトウェアで適用されます。

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 access-list *access-list-name*	IPv6 アクセス リスト名を定義し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3a	**deny** | **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]	**deny** または **permit** を入力して、条件が一致した場合にパケットを拒否するのか許可するのかを指定します。次に、条件について説明します。 • *protocol* には、インターネット プロトコルの名前（**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、または **udp**）、または番号（IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数）を入力します。ICMP、Transmission Control Protocol（TCP; 伝送制御プロトコル）、および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）の具体的なパラメータについては、ステップ 3b ～ 3d を参照してください。 • *source-ipv6-prefix*/*prefix-length* または *destination-ipv6-prefix*/*prefix-length* は、拒否または許可の条件を設定する送信元または宛先 IPv6 ネットワーク（またはネットワーク クラス）で、コロンで区切られた 16 ビット値を使用した 16 進数形式で指定されます（RFC 2373 を参照してください）。 **（注）** CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチは集約可能なグローバル ユニキャストおよびリンクローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および EUI ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合をサポートします。 • IPv6 プレフィクス ::/0 の省略形として **any** を入力します。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否または許可の条件を設定する発信元または宛先の IPv6 ホスト アドレスを、コロンで区切られた 16 ビット値を使用した 16 進数形式で入力します。 • （任意）*operator* には、指定のプロトコルの送信元または宛先ポートを比較するオペランドを指定します。オペランドは、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range** です。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が続く場合、送信元ポートと一致する必要があります。*destination-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が続く場合、宛先ポートと一致する必要があります。 • （任意）*port-number* 値は 0 ～ 65535 の範囲の 10 進数値か、TCP または UDP をフィルタリングするための TCP ポート名または UDP ポート名です。 • （任意）**dscp** *value* を入力して、各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント（DSCP）値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、非初期フラグメントを確認します。このキーワードは、プロトコルが **ipv6** の場合に限り表示されます。 • （任意）**log** を入力すると、エントリと一致するパケットを示すロギング メッセージがコンソールに送信されます。**log-input** を入力して、ログ エントリに入力インターフェイスを含めます。ロギングは、ルータ ACL に対してだけサポートされます。 • （任意）**sequence** *value* を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）**time-range** *name* を入力して、ステートメントの時間範囲を指定します。

	コマンド	目的
ステップ 3b	**deny** | **permit tcp** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示す任意のパラメータが追加されています。 • **ack** *:* 確認応答ビット設定。 • **established** *:* 確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • **fin**：終了ビット設定。送信元からのデータはこれ以上ありません。 • **neq** {*port* | *protocol*} *:* 指定のポート番号上にないパケットだけを照合します。 • **psh**：プッシュ機能ビット設定。 • **range** {*port* | *protocol*}：ポート番号範囲のパケットだけを照合します。 • **rst**：リセット ビット設定。 • **syn**：同期ビット設定。 • **urg** *:* 緊急ポインタ ビット設定。
ステップ 3c	**deny** | **permit udp** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] **[log]** [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**sequence** *value*] [**time-range** *name*]	（任意）UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、**udp** を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じですが、[*operator* [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP の場合、**established** パラメータは無効です。
ステップ 3d	**deny** | **permit icmp** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dscp** *value*] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 ICMP の場合は、**icmp** を入力します。ICMP パラメータはステップ 3a の IP プロトコルに関して説明されているパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。任意のキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプを基準にしてフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-code*：ICMP メッセージ コード タイプを基準にしてフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-message*：ICMP メッセージ タイプ名、または ICMP メッセージのタイプおよびコード名を基準にして、ICMP パケットをフィルタリングします。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 access-list	アクセス リスト コンフィギュレーションを確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定のアクセス リストから拒否または許可条件を削除するには、キーワードを指定して **no deny** | **permit** IPv6 アクセスリスト コンフィギュレーション コマンドを使用します。

次の例では、CISCO という IPv6 アクセス リストを設定します。リストの最初の拒否エントリは、5000 より大きい宛先 TCP ポート番号を持ったパケットをすべて拒否します。2 番めの拒否エントリは、5000 未満の送信元 UDP ポート番号を持ったパケットをすべて拒否します。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リストの最初の許可エントリは、すべての ICMP パケットを許可します。リストの 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 アクセス リストの末尾にあるので、この 2 番めの許可エントリが必要となります。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

インターフェイスへの IPv6 ACL の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する方法を説明します。ACL は、レイヤ 3 インターフェイスのアウトバウンドまたはインバウンド トラフィックに、あるいはレイヤ 2 インターフェイスのインバウンド トラフィックに適用できます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 インターフェイス（ルータ ACL 用）を指定し、インターフェイス コンフィギュレーション モードを開始します。 **（注）** IP ベース イメージが稼動しているスイッチは、ポート ACL をサポートしません。
ステップ 3	**no switchport**	ルータ ACL を適用する場合は、インターフェイスをレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変更します。
ステップ 4	**ipv6 address** *ipv6-address*	レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。 このコマンドは、レイヤ 2 インターフェイスでは、またはインターフェイスに明示的な IPV6 アドレスが設定されている場合には、必要ありません。
ステップ 5	**ipv6 traffic-filter** *access-list-name* {**in** | **out**}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。 **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	show **running-config**	アクセス リスト コンフィギュレーションを確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスからアクセス リストを削除するには、**no ipv6 traffic-filter** *access-list-name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、レイヤ 3 インターフェイスのアウトバウンド トラフィックにアクセスリスト *Cisco* を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

IPv6 ACL の表示

表 44-1 に示す 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

表 44-1　IPv6 アクセス リスト情報を表示するためのコマンド

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセス リストを表示します。
show ipv6 access-list [*access-list-name*]	設定済みのすべての IPv6 アクセス リスト、または名前で指定されたアクセス リストを表示します。

次の例では、**show access-lists** 特権 EXEC コマンドの出力を示します。出力では、スイッチに設定されたすべてのアクセス リストが表示されます。

```
Switch #show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次の例では、**show ipv6 access-lists** 特権 EXEC コマンドの出力を示します。出力には、スイッチに設定された IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30

IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```